UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

United States of America, Plaintiff, v. Kyle William Brenizer, Defendant.	Case No. 20-cr-177 (ECT/HB) **REPORT AND RECOMMENDATION**

HILDY BOWBEER, United States Magistrate Judge

This matter is before the Court on Defendant Kyle William Brenizer's Motion to Suppress Evidence Obtained by Search and Seizure [ECF No. 30], Motion to Suppress Evidence Obtained by Search and Seizure (Cell Phone Evidence) [ECF No. 59], and Motion to Suppress Evidence Obtained by Search and Seizure (Vehicle Evidence) [ECF No. 60]. The motions were referred to this Court for a report and recommendation pursuant to 28 U.S.C. § 636 and District of Minnesota Local Rule 72.1. For the reasons set forth below, the Court recommends that the motions be denied.

I. Background and Procedural History

An Indictment was filed against Defendant Kyle William Brenizer on August 19, 2020 [ECF No. 1], followed by a Superseding Indictment on February 9, 2021 [ECF No. 66], and a second Superseding Indictment on March 16, 2021 [ECF No. 76]. The second Superseding Indictment charges Brenizer with two counts of wire fraud, in violation of 18 U.S.C. § 1343; two counts of money laundering, in violation of 18 U.S.C. § 1957; and

three counts of aggravated identity theft, in violation of 18 U.S.C. § 1028A.

Brenizer challenged the admissibility of five categories of evidence in his motions to suppress: (1) electronic evidence obtained via subpoenas issued to TracFone Wireless, Inc., Verizon, and AT&T [ECF No. 30]; (2) evidence seized during a warrant-authorized search of Brenizer's residence on August 21, 2020 [ECF No. 30]; (3) email evidence obtained from Google pursuant to a search warrant [ECF No. 30]; (4) evidence obtained from a cell phone seized during the August 21, 2020, search of Brenizer's residence [ECF No. 59]; and (5) evidence seized from a 2017 GMC Sierra pursuant to a search warrant [ECF No. 60]. Brenizer represents in his post-hearing memorandum that his motion as to the first category is moot. (Def.'s Mem. Supp. Mots. Suppress at 2 [ECF 86].)

The Court held a hearing on the motions on June 10, 2021, at which the Government submitted the following exhibits:

- 7xx Van Buren Residence Search Warrant (Gov't's Ex. 1);
- 2017 GMC Sierra Search Warrant (Gov't's Ex. 2);
- Google Search Warrant (Gov't's Ex. 3);
- Items Seized 7xx Van Buren (Gov't's Ex. 4);
- Items Seized 2017 GMC Sierra (Gov't's Ex. 5); and
- Items Seized Google (Gov't's Ex. 6).

(Mot. Hr'g Ex. List [ECF No. 85].) Brenizer also submitted one exhibit: Cell Phone Extraction Report (Def.'s Ex. 7). No witnesses testified at the hearing.

Brenizer filed an omnibus post-hearing memorandum in support of his motions to suppress on June 24, 2021, and the Government filed its post-hearing memorandum in opposition on July 9, 2021. The Court took the motions under advisement on July 9, 2021.

II. Evidence Obtained from TracFone Wireless, Inc., Verizon, and AT&T

Brenizer represents in his post-hearing memorandum that his motion to suppress electronic evidence obtained via subpoenas issued to TracFone Wireless, Inc., Verizon, and AT&T is moot, in light of the Government's representations that it obtained only basic subscriber information and that it neither requested nor received historic cell cite location information. (Def.'s Mem. Supp. Mots. Suppress at 2.) Accordingly, the Court recommends that this aspect of Brenizer's Motion to Suppress Evidence Obtained by Search and Seizure [ECF No. 30] be denied as moot.

III. Evidence Obtained from Brenizer's Residence, Cell Phone, and Email Accounts

Internal Revenue Service (IRS) Special Agent Brian Pitzen submitted an affidavit in support of an application for a search warrant authorizing a search of Brenizer's residence at 7xx Van Buren Avenue in St. Paul, Minnesota. (*See* Gov't's Ex. 1.) United States Magistrate Judge Becky Thorson issued the warrant on August 19, 2020, and the warrant was executed two days later. Brenizer contends Special Agent Pitzen's affidavit did not provide probable cause to believe that a crime was committed, provide probable cause to believe that Brenizer committed the crime under investigation, or demonstrate a nexus between the residence and evidence of a crime. (Def.'s Mot. Suppress at 2; Def.'s Mem. Supp. Mots. Suppress at 3.)

Officers who executed the residential warrant seized a cell phone during the search, and Brenizer has filed a separate motion seeking to suppress evidence obtained from the phone. Brenizer argues that the affidavit did not provide probable cause for the

seizure or search of the phone, that the warrant did not meet the Fourth Amendment's particularity requirement, and that the warrant did not explicitly authorize the search and seizure of the cell phone. (Def.'s Mot. Suppress (Cell Phone Evidence) at 1–2, 4.)

Special Agent Pitzen submitted the same affidavit in support of an application for a search warrant directing Google to provide information from four email accounts associated with the following addresses: kyleb@true-cutconstruction.com, kbren5953@gmail.com, slabashcott@gmail.com, and kyle.w@interactiveinnovatorsinc.com. (Gov't's Ex. 3.) Magistrate Judge Thorson issued the warrant on August 19, 2020. Brenizer argues that the Google warrant lacked probable cause, was overbroad, and lacked particularity. (Def.'s Mem. Supp. Mots. Suppress at 8.)

A. Special Agent Pitzen's Affidavit

The following averments were set forth in Special Agent Pitzen's affidavit submitted in the applications for the 7xx Van Buren warrant and the Google warrant.

Brenizer formed the business True-Cut Construction, LLC (True-Cut), a home renovation contractor, in December 2015. (Gov't's Ex. 1 (Pitzen Aff. ¶ 11).) True-Cut did not report having any employees or paying any wages from 2016 through 2019. (*Id.* ¶ 12.) True-Cut's contractor license expired in December 2019. (*Id.* ¶ 13.)

An individual named "Kyle Williams" formed the corporation "Interactive Innovators" in January 1997. (*Id.* ¶ 14.) Interactive Innovators was dissolved in April 2005, then reinstated on April 23, 2000. (*Id.*) Brenizer has used the alias "Kyle Williams" on a LinkedIn page, which names "Kyle Williams" as the owner of both True-

Cut and Interactive innovators and displays a photograph of Brenizer. (*Id.* ¶ 15.)

On July 29, 2020, Special Agent Pitzen conducted surveillance at Brenizer's residence located at 7xx Van Buren Avenue in St. Paul, Minnesota, and saw a white male in a 2017 black GMC Sierra parked outside. (*Id.* ¶¶ 4(A), 17.) The agent conducted surveillance again on August 14, 2020. (*Id.* ¶ 17.) Both times, Special Agent Pitzen saw a white male who matched the photograph on Brenizer's Minnesota-issued identification card. (*Id.*)

The accountholder for Comcast high-speed internet service at 7xx Van Buren is "Kyle Williams," and the contact phone number is 612-345-xxxx. (*Id.* ¶ 18.) Brenizer paid for Comcast service in April and May 2020 at 7xx Van Buren in the name of "Kyle Williams" with funds from a Gate City bank account that is maintained in Brenizer's name. (*Id.* ¶ 48.)

Brenizer had three financial accounts at Gate City Bank for which he listed his employer as True-Cut and provided email addresses of kbren5953@gmail.com and kyleb@true-cutconstruction.com. (*Id.* ¶ 20.) Brenizer provided those two email addresses also on applications for a Brex Card and a Brex Cash Account for True-Cut on November 11, 2019, and on April 30, 2020. (*Id.* ¶ 21.)

Fifteen years after Interactive Innovators was dissolved, it was reinstated on April 23, 2020, with "Kyle Williams" listed as the Chief Executive Officer. (*Id.* ¶ 23.) Contemporaneous checking account records show that Brenizer made several payments to the Minnesota Secretary of State within days of the reinstatement. (*Id.*)

Brenizer submitted a Brex application for Interactive Innovators on April 30,

2020, providing the email kyle.w@interactiveinnovatorsinc.com. (*Id.* ¶ 22.) In support of that application, Brenizer provided a copy of the Articles of Incorporation for Interactive Innovators that named "Kyle Williams" as the director and 7xx Van Buren as the address for the contact information. (*Id.*) The IP address associated with 7xx Van Buren was used to log in to the Interactive Innovators Brex account on six dates in May and June 2020. (*Id.* ¶ 50.)

Brenizer submitted a PPP loan application on May 1, 2020, to BlueVine Capital Inc., for $841,000, for which he gave the email kyle.w@interactiveinnovatorsinc.com. (*Id.* ¶ 27.) The application stated that True-Cut's monthly payroll was $338,720 and that True-Cut employed 28 people. (*Id.* ¶ 28.) Brenizer provided a tax return indicating that True-Cut had paid $4,064,520 in wages in 2019, but the IRS had no such documentation. (*Id.*) Fake or altered bank statements for True-Cut were also provided to BlueVine. (*Id.* ¶ 29.) The IP address used to send records and information to BlueVine was assigned to 7xx Van Buren. (*Id.* ¶ 49.) BlueVine rejected the PPP loan application via an email sent to kyle.w@interactiveinnovatorsinc.com. (*Id.* ¶ 31.)

Brenizer submitted a second True-Cut loan PPP application to BlueVine on May 8, 2020, seeking the same amount of funds but omitting his name from the application. (*Id.* ¶ 33.) Instead, the application identified "Individual A" as True-Cut's owner and gave the email address slabashcott@gmail.com. (*Id.* ¶ 34.) On May 12, 2020, an application form with Individual A's name was signed and submitted to BlueVine Capital. (*Id.* ¶ 35.) The IP address used to send records and information to BlueVine is assigned to 7xx Van Buren. (*Id.* ¶ 49.) This time, the PPP loan application was

approved, and $841,000 was deposited into Brenizer's personal checking account at Gate City Bank. (*Id.* ¶¶ 36–37.) Prior to the deposit, the account balance was $15.57. (*Id.* ¶ 39.)

On May 16, 2020, Brenizer bought a motorcycle for $29,985.23, paid from his personal checking account at Gate City Bank. (*Id.* ¶ 40.) The check was returned as unpayable on May 21, 2020. (*Id.* ¶ 42.) Brenizer called Gate City Bank and asked why his account funds were frozen. (*Id.* ¶ 44.) He later tried to finance the motorcycle with a loan application submitted in the name of "Kyle Williams," which listed 7xx Van Buren as the address, kyle.w@interactiveinnovatorsinc.com as the email address, and 612-345-xxxx as the phone number. (*Id.*)

On May 19, 2020, Brenizer transferred $500,000 from his personal checking to the Brex account for Interactive Innovators. (*Id.* ¶ 41.) He later told Gate City Bank he had the PPP funds sent to his personal checking account because he did not have a business account. (*Id.* ¶ 44.)

According to Gate City Bank records, Brenizer has written checks for apparent rent payments for the 7xx Van Buren residence payable to "S.D." (*Id.* ¶ 46.) Special Agent Pitzen has seen the 2017 black GMC Sierra parked outside of 7xx Van Buren twice. (*Id.* ¶ 47.) The registered owner of the Sierra is "Individual A," whose name was used to submit the second PPP loan application. (*Id.*)

Based on all of the above, Special Agent Pitzen averred there was probable cause to believe that Brenizer

through entities he has operated and controlled—including True-Cut

> Construction LLC (True-Cut) and Interactive Innovators, Inc.—has engaged in a scheme to defraud lenders and the U.S. Small Business Administration (SBA) by applying for an $841,000 Payroll Protection Program (PPP) loan in the name of True-Cut based on material falsehoods and omissions.

(*Id.* ¶ 3.) According to Special Agent Pitzen, the investigation had revealed that, as part of the scheme, Brenizer used interstate wires and conducted monetary transactions involving the alleged fraud proceeds. (*Id.*) In addition, Special Agent Pitzen believed Brenizer had used his residence and four email accounts in furtherance of the scheme. (*Id.* ¶ 4.)

With specific respect to the 7xx Van Buren residence, Special Agent Pitzen believed evidence of the crimes under investigation, as described in Attachment B1 to the affidavit, would be located in the residence. (*Id.* ¶ 51.) Based on training and experience, he knows small businesses involved in construction and contracting commonly keep (1) records relating to sales and client transactions such as financial statements, correspondence, invoices, transaction dates, and letters; and (2) records relating to employees and business associates such as contact books, ledgers, invoices, emails, correspondence, and payments with whom Brenizer, "Kyle Williams," Individual A, True-Cut, or Interactive Innovators did business. (*Id.* ¶ 52.) He also knows that businesses maintain books and records to operate the business and track income and expenses; business maintain such records for a lengthy amount of time in places that are secure yet easily accessible; communicate via paper and emails, which are often stored on computers; and keep financial records such as loan applications electronically. (*Id.* ¶ 53–56.) Special Agent Pitzen believed that the documents sought by the warrant would be

stored on laptops and computers used by Brenizer, True-Cut Construction, and Interactive Innovators. (*Id.* ¶ 56.)

In regard to searches of any computers, based on his training and experience, Special Agent Pitzen believed the search would require the removal of computer devices to be processed later by a computer expert or in a controlled environment. (*Id.* ¶ 57.) The reason is that searching computers can take days or weeks, depending on the amount of data, and is highly technical. (*Id.* ¶ 57(a), (b).)

Regarding the email accounts, in addition to the information described above about the use of the accounts associated with the four identified email addresses in connection with the commission of the alleged crimes, Special Agent Pitzen knew, based on training and experience, that Google LLC's computers are likely to contain stored electronic communications and information about subscribers. (*Id.* ¶ 60.) A Google subscriber can also store files, addresses, contact lists, pictures, and has likely provided their full name, address, telephone number, and other identifiers. (*Id.* ¶ 61.) Account and email information may constitute evidence of the crimes under investigation because the account information can be used to identify the account's user. (*Id.*) In addition, email providers typically have records of the IP addresses used to register and log in to the account. (*Id.* ¶ 62.)

B. The 7xx Van Buren Search Warrant

In addition to Special Agent Pitzen's affidavit, the application for the 7xx Van Buren search warrant included Attachment A1, which described the property to be searched and contained three photographs of the home, and Attachment B1, which

described the particular items and information to be searched and seized. (Gov't's Ex. 1.) Attachment B1 narrowed the items to be searched to "evidence of violations of 18 U.S.C. §§ 1343 and 1957 and related offenses, occurring in 2019 and after[,] involving Kyle Brenizer a/k/a 'Kyle Williams,' Individual A, True[-]Cut Construction, LLC, or Interactive Innovators, Inc." (*Id.*) Within that narrowed scope, the particular items and information to be searched included documents and communications relating to the SBA or PPP, employment records, tax records, financial records, business records, computer hardware and software, and handwritten notes. (*Id.*)

Brenizer argues generally that Special Agent Pitzen's affidavit did not provide probable cause for the 7xx Van Buren warrant. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The task of a judge presented with an application for a search warrant is "to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

"Probable cause does not require evidence sufficient to support a conviction, nor even evidence demonstrating that it is more likely than not that the suspect committed a crime." *United States v. Fladten*, 230 F.3d 1083, 1085 (8th Cir. 2000) (cleaned up). Rather, "[i]n dealing with probable cause, however, as the very name implies, we deal

with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act." *Brinegar v. United States*, 338 U.S. 160, 175 (1949). When a defendant challenges the sufficiency of probable cause, "a reviewing court is to ensure that the issuing judge had a 'substantial basis' for concluding that probable cause existed, and we owe substantial deference to the determination of probable cause by the issuing judge." *United States v. LaMorie*, 100 F.3d 547, 552 (8th Cir. 1996). As part of the probable cause presentation, the affidavit submitted in support of a warrant must establish a "nexus . . . between the item to be seized and criminal behavior." *Warden v. Hayden*, 387 U.S. 294, 307 (1967). There must also be a nexus between the contraband and the place to be searched. *United States v. Tellez*, 217 F.3d 547, 550 (8th Cir. 2000).

The Court finds here that Special Agent Pitzen's affidavit provided probable cause to believe that evidence of a crime would be found in the 7xx Van Buren residence. The crimes under investigation were a scheme to defraud, violations of 18 U.S.C. § 1343 and § 1957, and related offenses. The facts and circumstances of the criminal activity under investigation were described extensively in the affidavit and demonstrated a fair probability that Brenizer applied for and obtained the $841,000 PPP loan based on falsehoods and omissions, involved True-Cut and Interactive Innovators in the alleged scheme to defraud, used interstate wires as part of the alleged scheme, and conducted or attempted to conduct monetary transactions using the proceeds. The nexus between the 7xx Van Buren residence and the crimes under investigation was established by, *inter alia*, averments that Brenizer lived at the residence and contracted for Comcast internet

service there and that the IP address for the Comcast account was used to provide allegedly fraudulent information to BlueVine and to log on to Interactive Innovators' Brex account. In addition, given the nature of the crimes under investigation and the nature of True-Cut's business, Special Agent Pitzen knew from his training and experience that the specific information and documents sought likely would be found in Brenizer's residence. Consequently, the Court recommends that evidence seized pursuant to the 7xx Van Buren search warrant not be suppressed for lack of probable cause.

C. The Cell Phone

Brenizer argues the seizure and search of the cell phone violated the Fourth Amendment's particularity requirement. He submitted a 48,835 pages "extraction report" that shows the phone contained information about his medications, personal relationships, family members, physical activity, location history, and communications with his lawyer. (*See* Def.'s Ex. 7; Def.'s Mem. Supp. Mots. Suppress at 5.) He contends the warrant did not authorize a seizure of or search for such information. Brenizer also points out that the warrant did not explicitly authorize the search and seizure of a cell phone.

A search warrant must describe with particularity the place to be searched and the items or persons to be seized. U.S. Const. amend IV; *see United States v. Horn*, 187 F.3d 781, 788 (8th Cir. 1999) ("To satisfy the particularity requirement of the fourth amendment, the warrant must be sufficiently definite to enable the searching officers to identify the property authorized to be seized."). The particularity requirement "is a standard of 'practical accuracy' rather than a hypertechnical one." *United States v.*

Peters, 92 F.3d 768, 769–70 (8th Cir. 1996). "The degree of specificity required in applying the particularity requirement is flexible and may vary depending on the circumstances and the types of items involved." *United States v. Kail*, 804 F.2d 441, 445 (8th Cir. 2011) (cleaned up). For a scheme to defraud, for example, "a search warrant is sufficiently particular in its description of the items to be seized if it is as specific as the circumstances and nature of activity under investigation permit." *Id.* (cleaned up).

Here, the warrant authorized the seizure of numerous items described in Attachment B1. The Court finds that Attachment B1 was quite particular in enumerating the items and information to be seized, and the list went on for more than three pages. Attachment B1 also narrowed the types of items and information to be seized to the crimes under investigation, to the relevant time frame, and to Brenizer and his companies. But neither Attachment B1 nor the warrant itself authorized the search or seizure of cell phones. Thus, the Court must consider whether the seizure and search of the cell phone exceeded the scope of the warrant.[1]

In *United States v. Pospisil*, No. 20-2375, 2021 WL 3046580 (8th Cir. July 20, 2021), the Eighth Circuit considered whether "evidence seized from [the defendant's] cell phone should have been suppressed because the warrant did not specifically include cell phones." *Id.* at *1. The court rejected the defendant's reliance on *Riley v. California*, 573 U.S. 373 (2014), because the cell phone search in *Riley* was a warrantless search, whereas the cell phone search in *Pospisil* was conducted pursuant to a warrant that

[1] To the extent Brenizer maintains his particularity argument, the Court finds the 7xx Van Buren warrant was sufficiently particular.

authorized the seizure and search of "electronic data processing and storage devices, computer[s,] and computer systems." *Pospisil*, 2021 WL 3046580, at *1. The court then assumed without deciding that the phone was outside the scope of the warrant and upheld the seizure and search of the phone under the *Leon* good faith exception to the exclusionary rule.[2] *Id.* at *2. Relying on *United States v. Suellentrop*, the court "conclude[d] that searching Pospisil's cell phone was at least 'among the objectively reasonable honest mistakes that the Fourth Amendment tolerates.'" *Id.* (quoting *Suellentrop*, 953 F.3d 1047, 1051 (8th Cir. 2020)).[3]

Brenizer makes a slightly different argument based on *Riley*: that the warrant should have made "note of the vast quantity of information typically contained [on cell phones] and of the sensitivity of that information." (Def.'s Mot. Suppress (Cell Phone Evidence) at 4.) The holding of *Riley* is inapposite here because, as noted in *Pospisil*, the search of the cell phone in *Riley* was conducted without a warrant. To the extent that

[2] "Under the *Leon* good-faith exception, disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good faith on the judge's determination that there was probable cause to issue the warrant." *United States v. Grant*, 490 F.3d 627, 632 (8th Cir. 2007). Courts have applied the good faith exception when the searching officers made an "honest mistake" in exceeding the scope of the warrant, *see United States v. Houck*, 888 F.3d 957, 960–61 (8th Cir. 2018) (quoting *Maryland v. Garrison*, 480 U.S. 79 (1987)); or acted in objective good faith in conducting the search, *United States v. Biles*, 100 F. App'x 484, 493–94 (6th Cir. 2004); *United States v. Gorman*, 104 F.3d 272, 275 (9th Cir. 1996).

[3] In *Suellentrop*, the Eighth Circuit determined that officers executing a search warrant "reasonably understood" the warrant to authorize a search of the defendant's cell phone because the warrant described the items to be searched as "DVDs, CDs, video cassettes, mass storage devices (i.e., hard drives, computers, jump drives, etc[.]) and photographs of victim(s)," as well as "computers, cameras, storage devices, and electronic devices." 953 F.3d at 1050.

Brenizer interprets *Riley* to stand for the proposition that a search warrant must explicitly acknowledge that cell phones contain vast amounts of sensitive information, that interpretation goes too far. Not only did *Riley* not address a search conducted pursuant to a warrant, but nothing in *Riley* suggests the actual warrant must acknowledge the quantity and sensitivity of information contained on a cell phone. Furthermore, as already noted, Attachment B1 to the search warrant narrowed the types of items and information to be seized to the crimes under investigation, to the relevant time frame, and to Brenizer and his companies. Finally, the Search Warrant Addendum further accounted for the sensitivity and quantity of information contained on electronic devices by instructing the government to avoid searching files and electronically stored information that were not described in the warrant and to establish a search methodology and "taint team" to ensure no attorney-client privileged communications would be reviewed inadvertently. (Gov't's Ex. 1 at 7.)

Turning to the *Leon* good faith exception, the 7xx Van Buren search warrant authorized the seizure and search of electronic documents and records, audio and video recorded messages, electronic media, electronic data processing and storage devices, and computers. These items are essentially the same as those described in the *Pospisil* warrant. But the Search Warrant Addendum here goes one step further: In authorizing the government to retain electronic storage devices seized pursuant to the warrant, it explicitly includes "smartphone" as such a device. (Gov't's Ex. 1 at 7.) *Riley* lends further support to the finding that a cell phone is a computer: "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also

happen to have the capacity to be used as a telephone." *Riley v. California*, 573 U.S. 373, 393 (2014). The Court concludes that it was not unreasonable for the officers who executed the warrant to believe the warrant authorized the seizure and search of Brenizer's cell phone.

Concerning the extent of information contained on the extraction report, Brenizer seems to take issue with the two-phase approach for the seizure and search of electronically stored information described in Federal Rule of Criminal Procedure 41(e)(2)(B). That Rule provides in relevant part: "A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B). The advisory committee's notes to the Rule explain:

> Computers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location. This rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.

Fed. R. Crim. P. 41(e)(2)(B) advisory committee's note to 2009 amendments. Given the time it would take at the location where a warrant is executed to "distinguish evidence of crimes from . . . more innocent electronic data and files," a practical and reasonable approach is to seize all of the electronic files and review them later. *United States v. Barnes*, No. 18-cr-120 (ADM/KMM), 2019 WL 3293467, at *10 (D. Minn. Apr. 8, 2019), *R. & R. adopted*, 2019 WL 2353659 (D. Minn. June 4, 2019).

Special Agent Pitzen described in his affidavit the process for searching computer systems. In his training and experience, evidence on computers must be downloaded, copied, or removed for later processing by an expert or in a controlled environment. (Pitzen Aff. ¶ 57.) The reason is the vast quantity of information that can be stored on computers, and searching and sorting the information can take weeks. (*Id.* ¶ 57(a).) The extraction report identifies Cellebrite, not the government, as the "physical analyzer." (Def.'s Ex. 7 at 1.) The files were extracted on September 25, 2020, approximately a month after the cell phone was seized. (*Id.*)

There is nothing in the extraction report that indicates the government deviated from Rule 41(e)(2)(B) or otherwise exceeded the scope of the warrant. Rather, it appears the extraction report was created by a third party, Cellebrite, that extracted information from the phone for law enforcement officers to review and determine what fell within the scope of the warrant. That process is specifically contemplated by Rule 41(e)(2)(B).

In sum, the Court finds no basis to recommend suppression of the evidence obtained from Brenizer's cell phone.

D. Emails

In addition to Special Agent Pitzen's affidavit, the search warrant application for the email accounts kyleb@true-cutconstruction.com, kbren5953@gmail.com, kyle.w@interactiveinnovatorsinc.com, and slabashcott@gmail.com included Attachment A2, which described the property to be searched as information for the four email accounts stored at premises controlled by Google. (Gov't's Ex. 3 at 2.) Attachment B2 narrowed the information to be disclosed by Google to the contents of all emails

associated with the accounts, information about the identification of the account and the account holder, the types of services that were utilized, contacts and calendar entries, pictures and files, and communications with Google about the accounts. (*Id.* at 3–4.) The information to be seized narrowed the above items further to evidence of violations of 18 U.S.C. §§ 1343 and 1957 and related offenses, that occurred in 2019, and that involved Brenizer, "Kyle Williams," Individual A, True-Cut, or Interactive Innovators. (Gov't's Ex. 3 at 4.) Within that narrowed scope, the information to be seized included documents related to the SBA or PPP, employment records, tax record, financial records, business records, funds provided by lenders, account information, the creator and user of the email accounts, access information, and emails that relate to the crimes under investigation. (*Id.* at 4–6.)

Brenizer argues generally that Special Agent Pitzen's affidavit did not provide probable cause to believe the email accounts would contain evidence of a crime. (Def.'s Mot. Suppress at 5.) The Court finds otherwise.

The affidavit described how Brenizer allegedly used each email address in furtherance of the crimes under investigation. Brenizer used the kbren5953@gmail.com and kyleb@true-cutconstruction.com email addresses for his Gate City Bank account and provided those two emails on PPP loan applications for True-Cut. Brenizer also provided those two email addresses on the Brex account applications for True-Cut. Brenizer provided the kyle.w@interactiveinnovatorsinc.com email address on his Interactive Innovators Brex application, first PPP loan application to BlueVine, and loan application for the motorcycle. And Brenizer allegedly provided the

slabashcott@gmail.com email address on his second PPP loan application to BlueVine. Additional details about how the subject email accounts were used to further the alleged scheme to defraud were set forth in paragraphs 19 through 50 of Special Agent Pitzen's affidavit. The Court concludes that the information contained in Special Agent Pitzen's affidavit established probable cause to believe that evidence of a crime would be contained within the four subject email accounts. Consequently, evidence seized pursuant to the Google warrant should not be suppressed.

IV. Evidence Seized from the 2017 Black GMC Sierra

Brenizer seeks to suppress evidence seized pursuant to a search warrant from a 2017 black GMC Sierra. Special Agent Pitzen provided a different affidavit in support of this application, but he also attached the applications submitted in support of the 7xx Van Buren and Google search warrants to this application. (*See* Gov't's Ex. 2 (Pitzen Aff. at 10).) Magistrate Judge Thorson issued the search warrant for the Sierra on August 21, 2020. (Gov't's Ex. 2.)

Special Agent Pitzen's affidavit summarily described the alleged scheme to defraud, wire fraud, and monetary transactions involving fraudulent proceeds. (Gov't's Ex. 2 (Pitzen Aff. ¶ 3).) In addition, very early in the morning on August 21, 2020, surveilling agents saw Brenizer arrive at the 7xx Van Buren residence in the Sierra. (*Id.* ¶ 6.) A team of law enforcement officers executed the 7xx Van Buren warrant later that day and found Brenizer hiding behind a basement wall. (*Id.* ¶¶ 6–7.) They did not find a computer. (*Id.* ¶ 7.) Brenizer's girlfriend told agents he was moving out of the residence that day. (*Id.* ¶ 8.) Agents on the scene looked in the windows of the Sierra and saw in

plain view a cell phone, computer bag, and other personal items. (*Id.* ¶ 9.)

Attachment A to the warrant identified the property to be searched as a 2017 black "GMV"[4] Sierra and attached yellow trailer and included the VINs for the Sierra and trailer. (Gov't's Ex. 2 at 2.) Attachment A also contained two photographs of the vehicle and trailer. Attachment B to the warrant described the items to be seized as evidence of violations of 18 U.S.C. §§ 1343 and 1957 and related offenses, that occurred in 2019, and that involved Brenizer, "Kyle Williams," Individual A, True-Cut, or Interactive Innovators. (*Id.* at 3.) Within that scope, the items to be seized consisted of documents and records related to the SBA and PPP, employment records, tax records, financial records, business records, funds provided by lenders, and account information. (*Id.* at 3–4.)

Brenizer moves to suppress evidence seized from the Sierra for three reasons. He first asserts the search was derivative of the purportedly unlawful search of 7xx Van Buren. (Def.'s Mot. Suppress (Vehicle Evidence) at 2 [ECF No. 60].) The Court has concluded, however, that the search of 7xx Van Buren was lawful and thus does not recommend suppression of evidence on that ground.

Brenizer next contends the affidavit did not provide probable cause to believe that a crime was committed or that he committed the crime. (Def.'s Mot. Suppress (Vehicle Evidence) at 3.) The Court concludes otherwise. Considering together Special Agent Pitzen's affidavit for the 7xx Van Buren and Google warrants, which was attached to and

[4] Brenizer does not challenge the typographical error on Attachment A.

incorporated by reference into the affidavit for the Sierra warrant, and Special Agent Pitzen's affidavit for the Sierra warrant, there was probable cause to believe that evidence of the crimes under investigation would be found in the Sierra. As recounted above, the crimes under investigation were a scheme to defraud, violations of 18 U.S.C. § 1343 and § 1957, and related offenses. The facts and circumstances of the alleged crimes were described extensively in Special Agent Pitzen's first affidavit and demonstrated a fair probability that Brenizer applied for and obtained the $841,000 PPP loan based on falsehoods and omissions, used interstate wires in doing so, and conducted or attempted to conduct monetary transactions using the proceeds. The nexus between the Sierra and the crimes under investigation was established by, *inter alia*, averments that Brenizer was observed driving the Sierra, that Brenizer used a computer and a phone in furtherance of the crimes under investigation, that no computer was found during a search of 7xx Van Buren, and that agents executing the 7xx Van Buren warrant saw in plain view a computer bag and cell phone in the Sierra. Given the facts and circumstances described in the two affidavits, the Court concludes there was probable cause to believe that evidence of the crimes under investigation would be found in the computer and phone that were located inside the Sierra.

Lastly, Brenizer argues the computer and phone should be suppressed because the Sierra warrant was an unconstitutional "general warrant" and lacked particularity. (Def.'s Mot. Suppress (Vehicle Evidence) at 4; Def.'s Mem. Supp. Mots. Suppress at 9.) To the contrary, Attachment B to the warrant described with particularity the scope and types of items to be seized. The items were limited by a description of the crimes under

investigation, to the year 2019, and by association with Brenizer, "Kyle Williams," Individual A, True-Cut, or Interactive Innovators. The items were further limited to documents and records related to the SBA or PPP, employment records, tax, records, financial records, business records, funds provided by lenders, and account information. Attachment B provided that the records and information sought could be stored electronically or, notably, on computers. The Court finds the Sierra warrant was sufficiently particular.

The Court rejects Brenizer's suggestion that the warrant lacked particularly or was overbroad simply because his computer, like his cell phone, could hold a wealth of information. As with the 7xx Van Buren warrant, a Search Warrant Addendum attached to the Sierra warrant accounted for the sensitivity and quantity of information contained on electronic devices by requiring the government to avoid searching files and electronically stored information that were not described in the warrant and to establish a search methodology and "taint team" to ensure no attorney-client privileged communications would be reviewed inadvertently.

To the extent Brenizer argues that the seizure of the phone was outside the scope of the Sierra warrant, the Court incorporates by reference its discussion in Part III.C and concludes that it was not unreasonable for the officers who executed the Sierra warrant to believe the warrant authorized the seizure of the phone.[5] With respect to the computer,

[5] Brenizer represents the phone seized from the Sierra has not been searched because it is inoperable. (Def.'s Mem. Supp. Mots. Suppress at 9 n.2.) Thus, at this time, there is no particular evidence obtained from the phone to suppress.

computers were explicitly listed in Attachment B to the warrant and thus fell within the warrant's scope.

In light of the above findings and conclusions, the Court recommends that Brenizer's motion to suppress evidence seized from the Sierra be denied.

Accordingly, based on the files, records, and proceedings herein, **IT IS HEREBY RECOMMENDED** that:

1. Defendant Kyle William Brenizer's Motion to Suppress Evidence Obtained by Search and Seizure [ECF No. 30] be **DENIED** in part and **DENIED AS MOOT** in part, as set forth fully above;
2. Defendant Kyle William Brenizer's Motion to Suppress Evidence Obtained by Search and Seizure (Cell Phone Evidence) [ECF No. 59] be **DENIED**; and
3. Defendant Kyle William Brenizer's Motion to Suppress Evidence Obtained by Search and Seizure (Vehicle Evidence) [ECF No. 60] be **DENIED**.

Dated: August 6, 2021

s/Hildy Bowbeer
HILDY BOWBEER
United States Magistrate Judge

NOTICE

Filing Objections: This Report and Recommendation is not an order or judgment of the District Court and is therefore not appealable directly to the Eighth Circuit Court of Appeals. Under D. Minn. LR 72.2(b)(1), "a party may file and serve specific written

objections to a magistrate judge's proposed finding and recommendations within 14 days after being served a copy" of the Report and Recommendation. A party may respond to those objections within 14 days after being served a copy of the objections. LR 72.2(b)(2). All objections and responses must comply with the word or line limits set forth in LR 72.2(c).

Under Advisement Date: This Report and Recommendation will be considered under advisement 14 days from the date of its filing. If timely objections are filed, this Report and Recommendation will be considered under advisement from the earlier of: (1) 14 days after the objections are filed; or (2) from the date a timely response is filed.